UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/064,943 | 08/30/2002 | Bastian Pochon | CH920010045US1 | 3630 |

29154 7590 12/22/2006

FREDERICK W. GIBB, III
GIBB INTELLECTUAL PROPERTY LAW FIRM, LLC
2568-A RIVA ROAD
SUITE 304
ANNAPOLIS, MD 21401

| EXAMINER | |
|---|---|
| MIRZA, ADNAN M | |
| **ART UNIT** | **PAPER NUMBER** |
| 2145 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 12/22/2006 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/064,943 | POCHON ET AL. | |
| | Examiner | Art Unit | |
| | Adnan M. Mirza | 2145 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *18-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *18-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

***Claim Rejections - 35 USC § 101***

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The subject matter "Computer Program Product" pertaining to claim 37 is not tangible.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 18-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (U.S. 6,279,113) and further in view of Spiegel (U.S. 6,954,765)

4. As per claims 18,37 Vaidya disclosed A method for normalization of traffic dare in a network comprising: fragmenting and reassembling packets of said data; dynamically establishing and maintaining a normalization table comprising said packets of said data; simultaneously transferring said packets of said data to a network intrusion detection system and a monitored end-system; and comparing said normalization table and identifiers of said packets of said data (col. 3, lines 13-27), said packets of said data are immediately forwarded

contemporaneously to said network intrusion detection system and to said monitored end system (col. 5, lines 33-39).

However Vaidya did not disclose in detail wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data

In the same field of endeavor Spiegel disclosed, "Valid handles for the copied sequence tables are written so that the copied sequence tables point to the appropriate original i.e. unaltered sequence tables and/or original fragments to complete the chains for the unaltered fragments. The original sequence tables and fragments that have been copied are deleted from storage. The deletion may occur by various mechanisms (col. 9, lines 11-17). The updating procedures may involve replacing data, i.e. overwriting, removing data, i.e. truncating or discarding, or adding data, i.e. amending. Fig. 4 is a flow chart showing one method of updating. A particular that contains old data to be changed is identified. The old data may be the entire contents of the fragment or only part of the data contained within the identified fragment (col. 8, lines 51-57).

It would have obvious to one having one ordinary skill in the art at the time of the invention was made to have incorporated Valid handles for the copied sequence tables are written so that the copied sequence tables point to the appropriate original i.e. unaltered sequence tables and/or original fragments to complete the chains for the unaltered fragments. The original sequence tables and fragments that have been copied are deleted from storage. The deletion may occur by

various mechanisms. The updating procedures may involve replacing data, i.e. overwriting, removing data, i.e. truncating or discarding, or adding data, i.e. amending. Fig. 4 is a flow chart showing one method of updating. A particular that contains old data to be changed is identified. The old data may be the entire contents of the fragment or only part of the data contained within the identified fragment as taught by Spiegel in the method of Vaidya to increase the perfomrace of the network by reducing network attack signature and so the network does have to spend more time creating new network attack signatures.

5. As per claims 19,31 Vaidya-Spiegel disclosed further comprising establishing information about said packet of said data without storing said data in said normalization table by extracting for each said identifier a header and calculating a length of said packet of said data, wherein said header indicates a length of said packet (Vaidya, col. 8, lines 39-56).

6. As per claims 20,32 Vaidya-Spiegel disclosed further comprising recording at least a partial receipt of said identifier by a sliding bit-mask which is moved to an offset, until said offset indicates receipt of all said data contained in said normalization table, wherein said receipt of said identifier is cleared after a time period which is selected equal or slightly higher than a lifetime of the last said packet inserted into said normalization table (Vaidya, col. 10, lines 57-67).

7. As per claim 21 Vaidya-Spiegel disclosed wherein a distance and a path MTU to said monitored end system in a network are monitored by said network intrusion detection system are measured and stored in said normalization table before the receipt of said packet of said data by said monitored end-system (Vaidya, col. 8, lines 39-56).

8. As per claim 22 Vaidya-Spiegel disclosed further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said monitored end-system, wherein when a contents of said TIME TO LIVE value is lower than a predetermined value, then said TIME TO LIVE value replaces said predetermined value; and wherein when said path MTU is lower than a size of the data packet a do not fragment FLAG is cleared (Vaidya, col. 10, lines 1-16).

9. As per claims 23,30 Vaidya-Spiegel disclosed A method for normalization of traffic data in a network comprising: fragmenting and reassembling packets of said data; dynamically establishing and maintaining a normalization table comprising said packets; simultaneously transferring said packets of said data to a network intrusion detection system and a monitored end-system; and comparing said normalization table and identifiers of said packets of said data (Vaidya, col. 3, lines 13-27), wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system (Spiegel, col. 8, lines 51-57), and wherein said dynamically establishing and monitoring comprises adding an aging bit to

all entries in said normalization table. wherein said aging bit is set whenever said entries are retrieved froze said normalization table (Vaidya, col. 5, lines 33-39).

10. As per claim 24 Vaidya-Spiegel disclosed wherein said dynamically establishing and maintaining further comprises periodically sequentially resetting after a time period aging bits previously reset (Vaidya, col. 9, lines 3-13).

11. As per claim 25 Vaidya-Spiegel disclosed wherein said dynamically establishing and maintaining comprises periodically sequentially probing after a second tune period, a distance and a path MTU to said monitored end-systems corresponding to said entries stored in said normalization table and updating said normalization table when said distance and said path MTU have changed (Vaidya, col. 8, lines 39-56).

12. As per claims 26,33 Vaidya-Spiegel disclosed further comprising establishing information about said packet of said data without storing said data in said normalization table by extracting for each said identifier a header and calculation a length of said packet of said data, wherein said header indicates a length of said packet (Vaidya, col. 8, lines 39-56).

13. As per claims 27,34,38 Vaidya-Spiegel disclosed further comprising recording at least a partial receipt of said identifier by a sliding bit-mask which is moved to an offset, until said offset indicates receipt of all said data contained in said normalization table, wherein said receipt

of said identifier is cleared after a time period which is selected equal or slightly higher than a lifetime of the last said packet inserted into said normalization table (Vaidya, col. 5, lines 33-39).

14. As per claims 28,35 Vaidya-Spiegel disclosed wherein a distance and a path MTU to said monitored end system in a network are monitored by said network intrusion detection system are measured and stored in said normalization table before the receipt of said packet of said data by said monitored end-system (Vaidya, col. 8, lines 39-56).

15. As per claims 29,36 Vaidya-Spiegel disclosed further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said monitored end-system, wherein when a contents of said TIME TO LIVE value is lower than a predetermined value, then said TIME TO LIVE replaces said predetermined value; and wherein when said path MTU is lower than a size of the data packet a do not fragment FLAG is cleared (Vaidya, col. 10, lines 1-16).

***Response to Arguments***

Applicant's arguments with respect to claims 18-38 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

16. Any inquiry concerning this communication or earlier communication from the examiner should be directed to Adnan Mirza whose telephone number is (571)-272-3885.

17. The examiner can normally be reached on Monday to Friday during normal business hours. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jason Cardone can be reached on (571)-272-3933. The fax for this group is (703)-746-7239. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

18. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for un published applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866)-217-9197 (toll-free).

AM

Adnan Mirza

Examiner

JASON CARDONE
SUPERVISORY PATENT EXAMINER